

| NODIS Library | Legal Policies(2000s) | Search |



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May
16, 2006
Expiration Date: May
16, 2011

[Printable Format \(PDF\)](#)

[Request Notification of Change](#) (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) |
[Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) | [Chapter11](#) |
[Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) | [Chapter16](#) | [Chapter17](#) |
[Chapter18](#) | [Chapter19](#) | [Chapter20](#) | [Chapter21](#) | [AppendixA](#) | [AppendixB](#) |
[ALL](#) |

SECTION V TECHNICAL CONTROLS

a. The technical controls focus on security controls that the IT system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization.

b. Technical controls are installed, maintained, and used by support and operations staff. This staff has the responsibility to create the user accounts, add users to access control lists, review audit logs for unusual activity, control bulk encryption over telecommunications links, and perform the countless operational tasks needed to use technical controls effectively. In addition, the support and operations staff provides needed input to the selection of controls based on their knowledge of system capabilities and operational constraints.

Chapter 19 Account Management

19.1 Identification and Authentication

19.1.1 Identification and authentication (I&A) is a critical building block of IT security. I&A is the basis for access control and a mechanism for establishing user accountability for NASA. I&A is a technical control to prevent unauthorized people or processes from gaining access to NASA information or information systems. The system must be able to

identify and differentiate among the diverse set of NASA users if access control is to work effectively. In addition, the approaches implemented must be compliant with Federal laws, regulations, and requirements.

19.1.2 Identification is a means by which a user provides a claimed identity to the system. Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors, requires the use of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors.

19.1.3 NASA information and information system owners are required to ensure that their applications, including COTS applications, are implemented utilizing FIPS 201 for identification, as well as to migrate their existing applications to use FIPS 201 following NASA's HSPD-12 Implementation Plan.

19.2 Account Management Requirements

19.2.1 NASA application and service providers are required to integrate their applications with the NASA account management and identity management systems. The NASA Account Management and Identity Management Systems will provide the NASA common infrastructure necessary to support the Federal E-Authentication and HSPD-12 requirements.

19.2.2 The NASA Account Management System (NAMS) will provide a central management system and repository of account information. This includes:

- a. A single Agency infrastructure to provide account management services and support.
- b. A reliable source of user access information for account provisioning.
- c. Elimination of duplicative user account information and administration.
- d. Enforcement of uniform security and auditing standards for account access.
- e. Termination of physical and logical access to IT resources promptly and reliably.
- f. A consistent process for establishing and managing accounts across all NASA Centers and installations.
- g. Definition of account management metrics in the system operations documentation.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) |
[Chapter5](#) | [Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) |
[Chapter11](#) | [Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) |
[Chapter16](#) | [Chapter17](#) | [Chapter18](#) | [Chapter19](#) | [Chapter20](#) |
[Chapter21](#) | [AppendixA](#) | [AppendixB](#) | [ALL](#) |

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
